Voice over Internet Protocol

Kristie Prinz

The Prinz Law Office

I. What is Voice over Internet Protocol ("VoIP")?

Voice over Internet Protocol ('VoIP") is a technology, which facilitates the transmission of voice communications over the Internet, instead of transmitting such communications over the more traditional public switched telephone network ("PSTN"). The technology works by converting an analog voice signal into a digital signal and then compressing it into Internet Protocol packets, which are then transmitted over the Internet.

VoIP technology may be accessed through (i) special VoIP phones that operate directly over the Internet without the use of a computer, (ii) an adapter designed to work with traditional phones, (iii) a computer directly, or (iv) a softphone, which connects directly to a computer without the use of hardware.

II. Why do lawyers need to know about VoIP?

Lawyers need to know about VoIP because of its widespread usage by companies and consumers—even law firms. To the user, VoIP service operates like a traditional PSTN phone service. However, from a legal perspective, VoIP laws are still developing, which is not the case with PSTN phone service, where the law is already well-developed.

III. What is different about using VoIP service from using a traditional PSTN phone service?

VoIP service has typically been more cost-effective than traditional PSTN phone services, which has made it an appealing alternative to PSTN service for many consumers and businesses. Some VoIP providers have offered free service to other members within their network, and others have offered flat fee services or bundled services with Internet service included for a discounted rate. In addition, VoIP service is a more portable service than traditional PSTN service, since the VoIP service is accessible anywhere that a high speed Internet connection is available and may be available in many locations where traditional PSTN phone service is unavailable. Finally, VoIP service allows users more flexibility with respect to selecting phone numbers than traditional PSTN service because the user does not have to be physically located in the area code for the particular phone number selected.

On the other hand, VoIP service has certain limitations. For example, if there is an Internet service outage or a power outage, VoIP service may not be available. VoIP users may run into quality of service and reliability issues, particularly when the network is congested or even when the VoIP service provider is not the same as their Internet

provider. They may also run into some problems sending faxes over their VoIP service. In addition, VoIP users may find that their VoIP service provider has not made directory assistance services available, or in the alternative, that their E911 service is ineffective in providing them assistance in an emergency, because service will be sent only to the emergency address on file for the particular user. VoIP users are also likely to run into more security issues with VoIP service than they did with their traditional PSTN service, given the fact that VoIP service is subject to all of the same security vulnerabilities that a computers would have in being connected to the Internet. Also, hackers and/or thieves have an additional incentive to attack VoIP service that does not exist in the case of Internet service: they can steal minutes and/or phone service.

IV. Who has the legal authority over VoIP services?

The Federal Communications Commission ("FCC") has taken the position that it has the authority to regulate VoIP services. The FCC has exercised its authority over VoIP on at least two occasions: first, the FCC ordered all VoIP service providers to comply with the Communications Assistance for Law Enforcement Act ("CALEA"), which is a law intended to preserve the ability of law enforcement to conduct electronic surveillance; and second, the FCC recently adopted a measure requiring VoIP providers to notify customers before discontinuing, reducing, or impairing their services. Additionally, the FCC recently sent a letter to Comcast, accusing it unfair VoIP practices, in subjecting third party VoIP services to "protocol agnostic" bandwidth throttling

In addition, Congress has passed one law to apply to VoIP technology: the New and Emerging Technologies 911 Improvement Act of 2008, which was signed into law by President Bush in July 2008. The Act was intended to ensure that Americans using VoIP services are able to dial 911 in an emergency.

States have attempted to exercise regulatory authority over VoIP on several occasions, particularly with respect to taxing VoIP services. Thus far, however, courts have held that the FCC pre-empts any state authority to regulate VoIP and struck down the states' efforts.

V. How is VoIP service regulated internationally?

The international legal and regulatory treatment of VoIP service varies considerably from country to country. While Canada's regulatory approach has been very similar to the approach taken in the United States, other countries such as Australia and Mexico have been much more proactive in applying the existing PSTN regulatory framework to VoIP service. Japan has taken a very hands-off approach to regulating VoIP, which accounts to some extent for the widespread popular adoption of the service. In contrast, countries such as China and Vietnam have placed heavy restrictions on VoIP service and service providers.

Because VoIP is a new technology, the international community has been grappling with many of the same legal issues that we have been dealing with in the United States, including but not limited to numbering and number portability, emergency

service access, network security, and law enforcement access. In addition, universal access has been an issue in many countries, where traditional PSTN phone access and Internet are not always available. These issues will continue to be addressed as VoIP technology becomes more commonly adopted.

VI. What are the key security vulnerabilities of VoIP?

VoIP technology is vulnerable in three key areas:

(a) Capture and Eavesdropping: With this type of security vulnerability, an eavesdropper identifies the VoIP packets as they travel through the network, copies them, and then reassembles them, in order to replay the conversations.

(b) Theft, including but not limited to toll fraud, identity theft, and registration hijacking. Toll fraud involves running up toll charges on a third party's account. Identity theft involves hijacking calls and taking on the identity of a third party, or in the alternative, modifying caller ID information in order to mislead someone as to the caller's identity. Registration hijacking involves the receipt and placement of calls to a third party's account.

(c) Denial of Service Attacks. This type of vulnerability involves the attack and disruption of the VoIP network, typically by flooding a VoIP component with signaling protocol packets, which eventually exhaust all of the resources of the device and result in the device performing poorly.

In addition, VoIP technology may be utilized to send hidden messages to a third party through the sound files. This practice is already being used by suspected terrorists to avoid attracting the attention of law enforcement.

VII. What legal liabilities arise from VoIP security vulnerabilities?

The legal liabilities arising from using VoIP are very similar to the legal liabilities of using a standard IT network. Companies risk losing trade secrets and/or confidential information through their VoIP systems, since confidential conversations may be subjected to eavesdropping. Companies also run the risk of being targeted for theft and for fraud, and they run the risk of violating privacy laws, if personal, third party information is disclosed through an attack on the VoIP network.

VIII. What best practices should companies adopt in order to secure their VoIP systems?

Companies should adopt the following best practices in order to secure their VoIP systems:

(a) Secure the overall IT network, including but not limited to utilizing firewalls, implementing an intrusion detection system, implementing an

intrusion prevention system, using antivirus protection, managing patches, and examining server logs.

(b) Use a private, non-routable IP address for the VoIP network: Instead of using a standard IP address, a Request for Comment ("RFC") 1918 Private IP address can be used, which is a special class of IP address intended for use internally within businesses. This IP address keeps the traffic local and off the Internet, which helps to ensure that the VoIP packets do not leave the organization.

(c) Encrypt the VoIP network: Use special IP handset phones on the VoIP network, which build an encrypted tunnel over the network.

(d) Use Virtual Private Networks when outside the corporate network, which provides an encrypted tunnel over the Internet.

(e) Educate employees using VoIP on good security practices, which may include advising them not to use unprotected VoIP networks such as Google Talk and Skype.

IX. Besides security, what other legal concerns should lawyers have about VoIP?

Lawyers should be concerned about the potential records retention implications of VoIP, since VoIP communications are electronic data just like email communications. A company may be faced with very expensive production requirements in discovery as a result of VoIP data. At the same time, the deletion or loss of VoIP data may constitute spoliation of evidence in some circumstances. Also, some laws require the retention of electronic records data, which could apply to VoIP data as well.

In addition, lawyers should also be concerned about the application of CALEA to VoIP. While in theory, wiretapping VoIP calls seems reasonable, the logistical reality of applying CALEA to VoIP is not so clear-cut. Because a VoIP network is built on the Internet, it is far more difficult to ensure the secure wiretap of a particular VoIP line than to secure a particular PSTN line. As a result, lawyers should be concerned about the vulnerabilities that wiretapping will introduce over the Internet, as well as the scope of information that the government will actually intercept in conducting such a wiretap.

X. Are there any hot topics in VoIP that technology lawyers are currently discussing?

The legal implications of using VoIP service in virtual worlds is the latest hot VoIP legal topic. Cyberspace lawyers have been debating for several years now the interesting legal implications raised by virtual worlds, since banking and legal systems were developing in these online societies, and virtual world issues had the potential to cross over into the "real" world. Now, a real life company, Vivox, has launched VoIP telephone service, which operates in a virtual world environment. Virtual world callers can dial out of the virtual world through phone booths and also can engage in voice chats online. The use of VoIP in virtual worlds raises some interesting legal questions. Does

the FCC have the authority to regulate VoIP calls made through virtual worlds? Does the new E911 law apply to VoIP calls made through virtual worlds, and if so, how do you comply in a virtual world? Does CALEA apply? The virtual world environment clearly adds an additional layer of complexity to the issues of regulating VoIP service, securing VoIP service, and wiretapping VoIP calls.